CLAIMS

What is claimed is:

1. In a network including at least one electronic device, a method of authentication of a web service customer, comprising:

a web server receiving a request for access to a first web service;

intercepting the request with an agent and collecting authentication credentials;

determining whether the web service customer is authenticated and authorized;

if the web service customer is authenticated and authorized, creating a session and session ticket;

returning an ID and the session ticket to the web server;

encrypting the session ticket ID and a public key into an assertion;

sending the assertion to the first web service; and

returning the assertion to the web service customer.

2. The method of claim 1, further comprising:

the web service customer inserting the assertion, and a signature into a document;

receiving a request for access to a second web service;

intercepting the request with the agent and collecting authentication credentials;

determining whether the assertion is valid;

if the assertion is valid, determining whether the web service customer is authenticated; and

if the web service customer is authenticated, granting the web service customer access to the second web service.

3. The method of claim 1, wherein the request comprises a SAML assertion.

4. The method of claim 1, wherein receiving a request comprises the web server receiving a public key and a request for access to a web service.

5. The method of claim 1, wherein intercepting the request comprises an XML agent intercepting the request and gathering authentication credentials.

6. The method of claim 1, wherein determining whether the web service customer is authenticated and authorized comprises comparing the web service customer with a database containing authentication and authorization data.

7. In a network including at least one electronic device, a method of authentication of a web service customer, comprising:

the web service customer inserting an assertion and a signature into a document;

a web server receiving a request for access to a web service;

intercepting the request with an agent and collecting authentication credentials;

determining whether the assertion is valid;

if the assertion is valid, determining whether the web service customer is authenticated; and

if the web service customer is authenticated, granting the web service customer access to the web service.

8. The method of claim 7, wherein the request comprises a SAML assertion.

9. In a network including at least one electronic device, a method of authentication of a web service customer, comprising:

the web service customer sending a request for access to a first web service;

a web server receiving an encrypted assertion and public key for incorporation into future requests; and

the web service customer being granted access to the first web service.

10. The method of claim 9, further comprising:

inserting the encrypted assertion and public key, and a signature, into a document;

requesting access to a second web service; and being granted access to the second web service.

11. The method of claim 9, wherein the request comprises a SAML assertion.

12. In a network including at least one electronic device, a method of authentication of a web service customer, comprising:

a web server receiving a request for access to a first web service;

intercepting the request and gathering authentication credentials;

determining whether the web service customer is authenticated and authorized;

if the web service customer is authenticated and authorized, creating a session and session ticket;

returning an ID and the session ticket to the web server;

encrypting the session ticket ID, a public key, and a private key into an assertion; and

sending the assertion to the first web service.

13. The method of claim 12, further comprising:

receiving a request from the first web service for access to a second web service;

intercepting the request with the agent and collecting authentication credentials;

determining whether the assertion is valid;

if the assertion is valid, determining whether the web service customer is authenticated; and

if the web service customer is authenticated, granting the first web service access to the second web service.

14. The method of claim 12, wherein the request comprises a SAML assertion.

15. The method of claim 12, wherein receiving a request comprises receiving an XML document without a public key.

16. The method of claim 12, wherein intercepting the request comprises an XML agent intercepting the request and gathering authentication credentials.

17. The method of claim 12, wherein determining whether the web service customer is authenticated and authorized comprises comparing the web service customer with a database containing authentication and authorization data.

18. In a network including at least one electronic device, a method of authentication of a source of a document, comprising:

a third party receiving a document from a previously authenticated first source;

the third party forwarding the document to a predetermined authentication system responsible for previously authenticating the first source to authenticate the source; and

the third party receiving an indication of validation as to whether the document originated with the first source.

19. The method of claim 18, wherein the request comprises a SAML assertion.

20. The method of claim 18, wherein receiving a document comprises a web server receiving a public key and a request for access to a web service.

21. The method of claim 18, wherein receiving a document comprises receiving an XML document without a public key.

22. The method of claim 18, wherein the predetermined authentication system comprises an XML agent intercepting the request and gathering authentication credentials.

23. The method of claim 22, wherein determining whether the document originated with the first source comprises comparing the first source with a database containing authentication and authorization data.